

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
20 September 2001 (20.09.2001)

PCT

(10) International Publication Number
WO 01/69556 A2

- (51) International Patent Classification²: G07F 19/00 (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.
- (21) International Application Number: PCT/US01/08209
- (22) International Filing Date: 15 March 2001 (15.03.2001)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
60/189,650 15 March 2000 (15.03.2000) US
- (71) Applicant: **MASTERCARD INTERNATIONAL INCORPORATED [US/US]**; 2000 Purchase Street, Purchase, NY 10577-2509 (US).
- (72) Inventors: **HOGAN, Edward, J.**; 14 N. Chatworth Avenue, Larchmont, NY 10538 (US). **CAMPBELL, Carl, M.**; 809 Malin Road, Newton Square, PA 19073 (US).
- (74) Agent: **SCHEINFELD, Robert, C.**; Baker Botts LLP, 30 Rockefeller Plaza, New York, NY 10112-0228 (US).
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

- without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.



WO 01/69556 A2

(54) Title: METHOD AND SYSTEM FOR SECURE PAYMENTS OVER A COMPUTER NETWORK

(57) Abstract: A method of conducting a financial transaction by a purchaser over a communications network is provided where the purchaser does not transmit his or her "real" payment card information over the network but instead secure payment application software is provided which allows for the transmission of a pseudo account number that is cryptographically processed for purposes of responding to an authorization request based on the real account number.

**METHOD AND SYSTEM FOR SECURE PAYMENTS
OVER A COMPUTER NETWORK**

SPECIFICATION

BACKGROUND OF INVENTION

5 This invention relates to a method and system for conducting secure financial transactions over a communications network and more particularly to a method and system for transmitting payments securely over a computer network, such as the Internet, and for transmitting sensitive information securely over public communication channels.

10 As is self-evident, on-line commerce has experienced tremendous growth over the last few years but even with that growth consumers are still troubled and concerned about using personal financial information and transmitting such information, such as credit card numbers and personal identification numbers, over public communications networks, such as the Internet. As a result, over the last few 15 years, companies have struggled to find a way -- the best way -- to ensure the security of payments made over a computer network and to decrease the risk of theft or misuse of financial information.

For example, U.S. Patent No. 5,883,810 entitled "Electronic Online Commerce Card With Transaction Proxy Number For Online Transactions" and 20 assigned to Microsoft Corporation, is directed to a system which provides for each transaction a temporary transaction number and associates it with the permanent account number; the transaction number looks like a real credit card number and the customer uses that transaction number and submits it to the merchant as a proxy for the customer account number. In this matter, the customer does not have to transmit 25 over a public network his or her real credit card number.

In the '810 patent, the merchant passes along the transaction number to the issuing institution, which in turn uses the transaction number as an index, accesses the real customer account number and processes the authorization, sending the

authorization reply back to the merchant under the transaction number. As a result, risk is purportedly minimized not only because the customer only transmits a transaction number but also because the proxy number is good only for a single purchase -- theft "would not greatly benefit a thief because it cannot be repeatedly used for other purchases or transactions." Col. 2, lines 60-61.

There is still a need to improve upon the prior art systems and in particular there is a need for a method and system for conducting a secure financial transaction over the Internet which avoids requiring the creation and transmission of a unique repeatedly generated transaction number to replace the transmission of the permanent account number for each conducted transaction.

SUMMARY OF THE INVENTION

According to the present invention, a "pseudo" account number is assigned to a customer and cryptographically linked to a consumer's payment account number. The payment account number is an account number issued by a financial institution or other organization that a consumer may use to make a payment for goods and/or services. For example, the payment account number may be the account number from a payment card, such as a credit or debit card, or from a payment application, such as an electronic cash application stored on a consumer's computer. The pseudo account number appears to be an actual payment account number to a merchant. That is, the pseudo account number has the same length as a valid payment account number and begins with a valid identification number (e.g., a "5" for MasterCard International Incorporated ("MasterCard")). The pseudo account number is used by the customer instead of the real account number for all of his or her on-line financial transactions.

All transactions based on pseudo account numbers are preferably cryptographically authenticated using a secret key that is unique for each account number. The authentication may be based on the private key of a public-key pair ("public-key authentication"), or based on a secret key other than a private key ("secret-key authentication"). Thus, if unauthorized persons were to ascertain any

pseudo account numbers, they would be unable to make fraudulent transactions using them.

BRIEF DESCRIPTION OF THE DRAWINGS

Further objects, features and advantages of the invention will become
5 apparent from the following detailed description taken in conjunction with the accompanying figures showing a preferred embodiment of the invention, on which:

FIG. 1 is a block diagram of the system for obtaining a secure payment application from a provider over the Internet in accordance with the invention;

10 FIG 2A is a block diagram of the system for conducting a secure payment over the Internet using the present invention with secret-key authentication of pseudo account numbers, in accordance with the invention;

FIG. 2B is a block diagram of the system for conducting a secure payment over the Internet using the present invention with public-key authentication of pseudo account numbers, in accordance with the present invention;

15 FIG. 3A is a block diagram illustrating the process preferably performed to obtain a pseudo account number for a given "real" account number, in accordance with the present invention;

20 FIG. 3B is a block diagram illustrating the process preferably performed to convert a pseudo account number back into its corresponding "real" account number;

FIGS. 4A and 4B illustrate the steps that are performed in accordance with the present invention when a card holder places an order with a merchant on the Internet and the merchant requests an authorization from an acquirer;

25 FIG. 5 is a block diagram illustrating the process of clearing a transaction in accordance with the present invention;

FIG. 6 is a block diagram illustrating exception processing in accordance with the present invention.

Throughout the figures, the same reference numerals and characters, unless otherwise stated, are used to denote like features, elements, components or portions of the illustrated embodiment. Moreover, while the subject invention will now be described in detail with reference to the figures, it is done so in connection with a preferred embodiment. It is intended that changes and modifications can be made to the described embodiment without departing from the true scope and spirit of the subject invention as defined by the appended claims.

10 DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Figure 1 illustrates an initial setup whereby a consumer who has, in this instance, a MasterCard financial transaction card decides to obtain a secure payment application from a secure payment application provider, such as MasterCard, over the Internet. The reader should understand that although there is repeated reference in the specification and Figures to MasterCard this is by way of example only.

As shown in Fig. 1, a provider, such as MasterCard (or an agent of MasterCard) has in its control one or more tamper-resistant security modules 10, which offer physical protection for the information stored inside the modules. These 20 security modules each contain the following secret keys: 1) one or more translation keys that are used to translate between pseudo account numbers and "real" account numbers; 2) if secret-key authentication is used, one or more derivation keys that are used to re-create the card-unique secret cryptographic keys; and 3) if public-key authentication is used, one or more provider "root" private keys. The process, then, 25 would preferably proceed as follows:

- The cardholder contacts MasterCard's web site via the Internet.
- The cardholder identifies himself/herself to MasterCard by providing, preferably under Secure Socket Layer (SSL) encryption known to those skilled in the art, the card account

number, card expiration date, and card verification code or CVC2 from his/her MasterCard card. CVC2 refers to authenticating information that is issued with some payment cards. These cards have the account number printed on the signature panel of the card followed by a three or four digit value. This value is generated by the issuing bank using a secret cryptographic key, and can be verified using this same key. Payment card brands have varying names for the value: MasterCard - Card Verification Code 2 (CVC2); American Express - Four-digit batch code (4DBC); and Visa - Card Verification Value 2 (CVV2). Supplying this value provides evidence that the person participating in a transaction had physical possession of the card at some point in time, because the value is not encoded on the magnetic stripe and thus not included in a normal transaction.

MasterCard verifies the CVC2 for the cards of those issuers for which MasterCard is provided (by secure means) the CVC2 keys. MasterCard may confirm the legitimacy of the other card data by obtaining a zero amount authorization from the issuer. MasterCard may obtain this authorization over its Banknet™ communications network.

After MasterCard has confirmed the legitimacy of the cardholder-provided card data, the secure payment application software is made available to the cardholder and may be downloaded over the Internet under SSL encryption. The software includes a secret cryptographic key that is unique to this card. If secret-key authentication is used, the secret key is preferably determinable from the card's "real" account number (i.e., the actual card payment account number issued by the cardholder's issuing bank). If public-key authentication is used, MasterCard provides a certificate that links the real

- account number with the corresponding public key, which certificate is signed by a MasterCard “root” private key. The software also includes the cardholder’s “real” account number, and a “pseudo” account number that MasterCard may relate to the “real” account number.
- 5
- The cardholder may provide a password to MasterCard prior to downloading the secure payment application or may select a password when the secure payment application is being installed on the cardholder's computer. If a password is provided or selected, the cardholder will thereafter be required to enter this password in order to activate the secure payment application.
- 10
- If secret-key authentication is used, the card-unique secret key may be cryptographically computed from the card's “real” account number using a higher-level secret cryptographic key that is common to many or all account numbers. The higher-level secret cryptographic key preferably resides solely within physically-secure and tamper-resistant hardware devices (referred to as “security modules”) that are controlled by
- 15
- MasterCard or by acquirer institutions. If the secure payment application includes a card-unique private key (for public-key authentication), the associated certificate is signed using a MasterCard private “root” key that resides only in a relatively few security modules that are controlled directly by MasterCard or by trusted agents to whom MasterCard has delegated this certificate-signing function.
- 20
- The pseudo account number has the same length as the “real” account number, consists solely of decimal digits, and begins with a valid identification number (e.g., a “5” for MasterCard). Therefore, the pseudo account number will appear to be a valid account number to merchants.
- 25
-
- 30

- In order for an acquirer or MasterCard to be able to differentiate between a “real” account number and a pseudo account number, there must be an indication in the account number or in the transaction record of the type of account number being used. In one embodiment of the present invention, this indication is provided in the second digit of the pseudo account number, which acts as a special identifier. For example, for MasterCard cards, the second digit of an account number may be made a “9” to indicate a pseudo account number. In this case, the 16th digit of the account number, which is normally a check digit used to detect manual entry errors, is deleted to make room for the additional second digit.
- In some cases, it may be possible that the transaction record may include data indicating that the account number is a pseudo account number.
- MasterCard may periodically update the secure payment application.
- If secret-key authentication is used, the following steps may be performed within a security module controlled by MasterCard or one of its agents to obtain a card-unique secret key to be included in the MasterCard secure payment application. The following steps assume the use of the DEA (Data Encryption Algorithm, which is a U.S. Government standard cryptographic algorithm) with a double-length key. They also assume that the MasterCard security module holds a secret high-level key called the Per-Card Key Derivation Key that consists of 16 bytes and is used with many or all card account numbers to cryptographically compute a card-unique secret key, called the Per-Card Key, given the card’s 16-digit payment account number. The steps are:

1. Considering the payment account number as 16 binary-coded-decimal digits of 4 bits each, DEA-encrypt these 64 bits using as the encryption key the left-most 8 bytes of the 16-byte Per-Card Key Derivation Key.
2. DEA-decrypt the result of Step 1 using as the decryption key the right-most 8 bytes of the 16-byte Per-Card Key Derivation Key.
5
3. DEA-encrypt the result of Step 2 using as the encryption key (again) the left-most 8 bytes of the 16-byte Per-Card Key Derivation Key.
4. Use the result of Step 3 as the left-most 8 bytes of the unique Per-Card Key.
10
5. DEA-encrypt the result of Step 3 using as the encryption key the left-most 8 bytes of the 16-byte Per-Card Key Derivation Key.
6. DEA-decrypt the result of Step 5 using as the decryption key the right-most 8 bytes of the 16-byte Per-Card Key Derivation Key.
15
7. DEA-encrypt the result of Step 6 using as the encryption key (again) the left-most 8 bytes of the 16-byte Per-Card Key Derivation Key.
8. Use the result of Step 7 as the right-most 8 bytes of the 16-byte unique Per-Card Key, and place this key in the secure payment application in such a way that it will not be disclosed during the normal operation of this application.
20
- If public-key authentication is used, the following steps may be performed within a security module controlled by MasterCard or one of its agents to provide a card-unique private key and a card-unique certificate for the corresponding public key, which private key and certificate are to be included in the MasterCard secure payment application:
25
1. For a recognized public-key algorithm (e.g. RSA, Elliptic Curve), compute a unique private key and the corresponding public key using established security procedures.

2. Using a recognized secure hash algorithm (e.g. SHA-1), hash, for example, (1) the just-generated public key for the card in question, (2) the pseudo account number for this card, (3) an appropriate date (to be optionally used to determine certificate expiration) and (4) the identity of the current MasterCard “root” key (in the event that this key should change).
- 5 3. Using a recognized public key algorithm, and a MasterCard “root” private key, create a digital signature on the result of Step 2 (with appropriate padding).
- 10 4. In the per-card secure payment application, place the just-generated private key in such a way that it cannot be disclosed in normal operation. Also place in this secure payment application a digital certificate consisting of (for example) (1) the card-unique public key, (2) the card’s pseudo account number, (3) the above-indicated date, (4) the identity of the MasterCard “root” key used to sign the certificate, and (4) the above-described digital signature.
- 15

Figure 2a is a diagram of a system for conducting a secure payment over the Internet using the present invention with secret-key authentication of pseudo account numbers.

20 As shown in Fig. 2a, an acquirer 12 has in its control one or more tamper-resistant security modules, which offer physical protection for the information stored inside the modules. These security modules each contain one or more secret keys, the translation key or keys, that are used to translate between pseudo account numbers and “real” account numbers. Each of these modules also contain one or more
25 higher-level secret keys, called the derivation key or keys, that are used to re-create the card-unique secret cryptographic keys.

The modules may be provided by MasterCard to the acquirer and may function similarly to the security modules currently installed in banks that operate Cirrus automatic teller machines (ATMs). MasterCard provides to the acquirer a

security specification and/or software application, which the acquirer may make available to merchants that desire to accept MasterCard cards with pseudo account numbers. Although it is preferred for an acquirer to have a security module, it is not required. If a security module is not provided to an acquirer, the acquirer will be 5 required to forward all pseudo account numbers to MasterCard for translation and authentication.

Figure 2B is a diagram of a system for conducting a secure payment over the Internet using the present invention with public-key authentication of pseudo account numbers. As shown in Fig. 2b, the only significant difference with Figure 2a 10 is that a public-key pair is utilized. Like before, the acquirer 12 has in its control one or more tamper-resistant security modules 10, which offer physical protection for the information stored inside the modules. These security modules each contain one or more secret keys, i.e., the translation key or keys, that are used to translate between pseudo account numbers and “real” account numbers. Like above, the modules are 15 provided by MasterCard to the acquirer and may function similarly to the security modules currently installed in banks that operate Cirrus automatic teller machines (ATMs). MasterCard provides to the acquirer a security specification and/or software application, which the acquirer may make available to merchants that desire to accept MasterCard cards with pseudo account numbers. Although it is preferred for an 20 acquirer to have a security module, it is not required. If a security module is not provided to an acquirer, the acquirer will be required to forward all pseudo account numbers to MasterCard for translation and authentication.

Figure 3 illustrates the process that may be performed within a security module to obtain the pseudo account number for a given “real” account number. The 25 process utilizes the DEA with a double-length key. It is assumed that the security module holds a secret high-level key (the Account Number Translation Key) that consists of 16 bytes and is used with many or all card account numbers to obtain the pseudo account number that corresponds to each. It is assumed that the first three digits of the “real” account number occur unchanged in the pseudo account number 30 with the digit “9” inserted between the first and second digits, and that the 16th digit

(the check digit) of the “real” account number is ignored. The twelve digits from Digit 4 through Digit 15 of the “real” account number are encrypted and become digits 5 through 16 of the pseudo account number. This encryption is illustrated as function “E1” in Fig. 3a. This encryption method may use a methodology known as 5 ‘DESX’ to maintain high security while minimizing the number of DEA operations that are required. The following defines possible steps to achieve the encryption:

1. Select the 6 digits from positions 4 through 9 of the “real” account number (the 6 left-most of the 12 account-number digits to be encrypted). Represent each digit as a 4-bit binary-coded decimal value.
- 10 2. Left-justify the 24 bits produced by Step 1 in a 64-bit field, where the 37 bits to the immediate right of these bits are all set to binary zero, and the three right-most bits of the 64-bits are set to binary ‘001’.
3. Exclusive-or the result of Step 2 with the left-most 8 bytes (64 bits) of the Account Number Translation Key.
- 15 4. DEA encrypt the result of Step 3 using as the key the right-most 8 bytes of the Account Number Translation Key.
5. Exclusive-or the result of Step 4 with (again) the left-most 8 bytes (64 bits) of the Account Number Translation Key.
6. Consider the result of Step 5 as 16 hexadecimal digits. Starting with the 20 left-most digit, select those digits with the value of ‘9’ or less until 6 such digits (from the binary set ‘0000’ through ‘1001’, decimal 0 through 9) have been selected. If fewer than 6 such digits were found, select the remaining digits by re-scanning the result of the Step 5, this time selection only those 4-bit digits with a value greater than binary ‘1001’ (decimal ‘9’), and subtract binary ‘1010’ (decimal ‘10’) from each. This process produces 6 binary-coded-decimal digits.
- 25 7. Select the 6 digits from positions 10 through 15 of the “real” account number (the 6 right-most of the 12 account-number digits to be encrypted). Represent each digit as a 4-bit binary-coded decimal value.

Mod-10 add each of these 6 binary-coded-decimal digits to the corresponding binary-coded-decimal digit resulting from Step 6.

8. Left-justify the 24 bits produced by Step 7 in a 64-bit field, where the 37 bits to the immediate right of these bits are all set to binary zero, and the three right-most bits of the 64-bits are set to binary '010'.
5
9. Exclusive-or the result of Step 8 with the left-most 8 bytes (64 bits) of the Account Number Translation Key.
10. DEA encrypt the result of Step 9 using as the key the right-most 8 bytes of the Account Number Translation Key.
10
11. Exclusive-or the result of Step 10 with (again) the left-most 8 bytes (64 bits) of the Account Number Translation Key.
12. Consider the result of Step 11 as 16 hexadecimal digits. Starting with the left-most digit, select those digits with the value of '9' or less until 6 such digits (from the binary set '0000' through '1001', decimal 0 through 9) have been selected. If fewer than 6 such digits were found, select the remaining digits by re-scanning the result of Step 11, this time selection only those 4-bit digits with a value greater than binary '1001' (decimal '9'), and subtract binary '1010' (decimal '10') from each. This process produces 6 binary-coded-decimal digits.
15
13. Mod-10 add each of the 6 binary-coded-decimal digits resulting from Step 12 to the corresponding binary-coded-decimal digit resulting from Step 1.
20
14. Left-justify the 24 bits produced by Step 13 in a 64-bit field, where the 37 bits to the immediate right of these bits are all set to binary zero, and the three right-most bits of the 64-bits are set to binary '011'.
25
15. Exclusive-or the result of Step 14 with the left-most 8 bytes (64 bits) of the Account Number Translation Key.

16. DEA encrypt the result of Step 15 using as the key the right-most 8 bytes of the Account Number Translation Key.
17. Exclusive-or the result of Step 16 with (again) the left-most 8 bytes (64 bits) of the Account Number Translation Key.
- 5 18. Consider the result of Step 17 as 16 hexadecimal digits. Starting with the left-most digit, select those digits with the value of '9' or less until 6 such digits (from the binary set '0000' through '1001', decimal 0 through 9) have been selected. If fewer than 6 such digits were found, select the remaining digits by re-scanning the result of Step 17, this time selection only those 4-bit digits with a value greater than binary '1001' (decimal '9'), and subtract binary '1010' (decimal '10') from each. This process produces 6 binary-coded-decimal digits.
- 10 19. Mod-10 add each of the 6 binary-coded-decimal digits resulting from Step 18 to the corresponding binary-coded-decimal digit resulting from Step 7.
- 15 20. Left-justify the 24 bits produced by Step 19 in a 64-bit field, where the 37 bits to the immediate right of these bits are all set to binary zero, and the three right-most bits of the 64-bits are set to binary '100'.
21. Exclusive-or the result of Step 20 with the left-most 8 bytes (64 bits) of the Account Number Translation Key.
- 20 22. DEA encrypt the result of Step 21 using as the key the right-most 8 bytes of the Account Number Translation Key.
23. Exclusive-or the result of Step 22 with (again) the left-most 8 bytes (64 bits) of the Account Number Translation Key.
- 25 24. Consider the result of Step 23 as 16 hexadecimal digits. Starting with the left-most digit, select those digits with the value of '9' or less until 6 such digits (from the binary set '0000' through '1001', decimal 0 through 9) have been selected. If fewer than 6 such digits were found, select the remaining digits by re-scanning the result of Step 23, this time

selection only those 4-bit digits with a value greater than binary ‘1001’ (decimal ‘9’), and subtract binary ‘1010’ (decimal ‘10’) from each. This process produces 6 binary-coded-decimal digits.

25. Mod-10 add each of the 6 binary-coded-decimal digits resulting from Step 24 to the corresponding binary-coded-decimal digit resulting from Step 13.
- 5 26. Left-justify the 24 bits produced by Step 25 in a 64-bit field, where the 37 bits to the immediate right of these bits are all set to binary zero, and the three right-most bits of the 64-bits are set to binary ‘101’.
- 10 27. Exclusive-or the result of Step 26 with the left-most 8 bytes (64 bits) of the Account Number Translation Key.
28. DEA encrypt the result of Step 27 using as the key the right-most 8 bytes of the Account Number Translation Key.
- 15 29. Exclusive-or the result of Step 28 with (again) the left-most 8 bytes (64 bits) of the Account Number Translation Key.
30. Consider the result of Step 29 as 16 hexadecimal digits. Starting with the left-most digit, select those digits with the value of ‘9’ or less until 6 such digits (from the binary set ‘0000’ through ‘1001’, decimal 0 through 9) have been selected. If fewer then 6 such digits were found, select the remaining digits by re-scanning the result of Step 29, this time selection only those 4-bit digits with a value greater than binary ‘1001’ (decimal ‘9’), and subtract binary ‘1010’ (decimal ‘10’) from each. This process produces 6 binary-coded-decimal digits.
- 20 31. Mod-10 add each of the 6 binary-coded-decimal digits resulting from Step 30 to the corresponding binary-coded-decimal digit resulting from Step 19.
- 25 32. Concatenate left-to right (1) four decimal digits consisting of the left-most 3 decimal digits of the “real” account number with the digit ‘9’ inserted between the first and second digit, with (2) the 6 decimal digits

resulting from Step 25, with (3) the 6 decimal digits resulting from Step 31. Use the resulting 16 decimal digits as the pseudo account number.

Figure 3b illustrates the process performed by a security module in the acquirer's facility to convert a pseudo account number (created from a "real" account number using the procedure described in Figure 3a) back into its corresponding "real" account number. The process utilizes the DEA with a double-length key. It is assumed that the security module holds a secret high-level key (the Account Number Translation Key) that consists of 16 bytes and is used with many or all card account numbers to obtain the pseudo account number from "real" account numbers and vice-versa. It is assumed that the first three digits of the "real" account number occur unchanged in the pseudo account number with the digit "9" inserted between the first and second digits, and that 16th digit (the check digit) of the "real" account number is not included in the pseudo account number. Therefore to convert from a pseudo account number to a "real" account number it is necessary to decrypt Digit 5 through Digit 16 of the pseudo account number to provide Digit 4 through Digit 15 of the "real" account number. The decryption is illustrated as function "D1" in Fig. 3b. Digit 1 through Digit 3 of the "real" account number are obtained from Digit 1 through Digit 4 of the pseudo account number by discarding the second digit (always a '9'). Finally, the 16th digit of the "real" account number must be computed from the other 15 digits by applying an appropriate check-digit-generation algorithm. The translation process is as follows:

1. Select the 6 digits from positions 5 through 10 of the pseudo account number (the 6 left-most of the 12 pseudo account-number digits to be decrypted). Represent each digit as a 4-bit binary-coded decimal value.
- 25 2. Left-justify the 24 bits produced by Step 1 in a 64-bit field, where the 37 bits to the immediate right of these bits are all set to binary zero, and the three right-most bits of the 64-bits are set to binary '101'.
3. Exclusive-or the result of Step 2 with the left-most 8 bytes (64 bits) of the Account Number Translation Key.

4. DEA encrypt the result of Step 3 using as the key the right-most 8 bytes of the Account Number Translation Key.
5. Exclusive-or the result of Step 4 with (again) the left-most 8 bytes (64 bits) of the Account Number Translation Key.
- 5
10 6. Consider the result of Step 5 as 16 hexadecimal digits. Starting with the left-most digit, select those digits with the value of '9' or less until 6 such digits (from the binary set '0000' through '1001' (decimal 0 through 9) have been selected. If fewer than 6 such digits were found, select the remaining digits by re-scanning the result of the Step 5, this time selection only those 4-bit digits with a value greater than binary '1001' (decimal '9'), and subtract binary '1010' (decimal '10') from each. This process produces 6 binary-coded-decimal digits.
7. Select the 6 digits from positions 11 through 16 of the pseudo account number (the 6 right-most of the 12 account-number digits to be decrypted). Represent each digit as a 4-bit binary-coded decimal value. From each of these 6 binary-coded-decimal digits, subtract the corresponding binary-coded-decimal digit resulting from Step 6.
8. Left-justify the 24 bits produced by Step 7 in a 64-bit field, where the 37 bits to the immediate right of these bits are all set to binary zero, and the three right-most bits of the 64-bits are set to binary '100'.
- 20
15 9. Exclusive-or the result of Step 8 with the left-most 8 bytes (64 bits) of the Account Number Translation Key.
10. DEA encrypt the result of Step 9 using as the key the right-most 8 bytes of the Account Number Translation Key.
- 25
11. Exclusive-or the result of Step 10 with (again) the left-most 8 bytes (64 bits) of the Account Number Translation Key.
12. Consider the result of Step 11 as 16 hexadecimal digits. Starting with the left-most digit, select those digits with the value of '9' or less until 6 such digits (from the binary set '0000' through '1001', decimal 0

through 9) have been selected. If fewer than 6 such digits were found, select the remaining digits by re-scanning the result of Step 11, this time selection only those 4-bit digits with a value greater than binary '1001' (decimal '9'), and subtract binary '1010' (decimal '10') from each. This process produces 6 binary-coded-decimal digits.

5

13. Mod-10 subtract each of the 6 binary-coded-decimal digits resulting from Step 12 from the corresponding binary-coded-decimal digit resulting from Step 1.
14. Left-justify the 24 bits produced by Step 13 in a 64-bit field, where the 10 37 bits to the immediate right of these bits are all set to binary zero, and the three right-most bits of the 64-bits are set to binary '011'.
15. Exclusive-or the result of Step 14 with the left-most 8 bytes (64 bits) of the Account Number Translation Key.
16. DEA encrypt the result of Step 15 using as the key the right-most 8 15 bytes of the Account Number Translation Key.
17. Exclusive-or the result of Step 16 with (again) the left-most 8 bytes (64 bits) of the Account Number Translation Key.
18. Consider the result of Step 17 as 16 hexadecimal digits. Starting with the left-most digit, select those digits with the value of '9' or less until 20 6 such digits (from the binary set '0000' through '1001', decimal 0 through 9) have been selected. If fewer than 6 such digits were found, select the remaining digits by re-scanning the result of Step 17, this time selection only those 4-bit digits with a value greater than binary '1001' (decimal '9'), and subtract binary '1010' (decimal '10') from each. This process produces 6 binary-coded-decimal digits.
- 25 19. Mod-10 subtract each of the 6 binary-coded-decimal digits resulting from Step 18 from the corresponding binary-coded-decimal digit resulting from Step 7.

20. Left-justify the 24 bits produced by Step 19 in a 64-bit field, where the 37 bits to the immediate right of these bits are all set to binary zero, and the three right-most bits of the 64-bits are set to binary '010'.
21. Exclusive-or the result of Step 20 with the left-most 8 bytes (64 bits) of the Account Number Translation Key.
5
22. DEA encrypt the result of Step 21 using as the key the right-most 8 bytes of the Account Number Translation Key.
23. Exclusive-or the result of Step 22 with (again) the left-most 8 bytes (64 bits) of the Account Number Translation Key.
- 10 24. Consider the result of Step 23 as 16 hexadecimal digits. Starting with the left-most digit, select those digits with the value of '9' or less until 6 such digits (from the binary set '0000' through '1001', decimal 0 through 9) have been selected. If fewer than 6 such digits were found, select the remaining digits by re-scanning the result of Step 23, this time selection only those 4-bit digits with a value greater than binary '1001' (decimal '9'), and subtract binary '1010' (decimal '10') from each. This process produces 6 binary-coded-decimal digits.
15
25. Mod-10 subtract each of the 6 binary-coded-decimal digits resulting from Step 24 from the corresponding binary-coded-decimal digit resulting from Step 13.
20
26. Left-justify the 24 bits produced by Step 25 in a 64-bit field, where the 37 bits to the immediate right of these bits are all set to binary zero, and the three right-most bits of the 64-bits are set to binary '001'.
27. Exclusive-or the result of Step 26 with the left-most 8 bytes (64 bits) of the Account Number Translation Key.
25
28. DEA encrypt the result of Step 27 using as the key the right-most 8 bytes of the Account Number Translation Key.

29. Exclusive-or the result of Step 28 with (again) the left-most 8 bytes (64 bits) of the Account Number Translation Key.
30. Consider the result of Step 29 as 16 hexadecimal digits. Starting with the left-most digit, select those digits with the value of '9' or less until 6 such digits (from the binary set '0000' through '1001', decimal 0 through 9) have been selected. If fewer than 6 such digits were found, select the remaining digits by re-scanning the result of Step 23, this time selection only those 4-bit digits with a value greater than binary '1001' (decimal '9'), and subtract binary '1010' (decimal '10') from each. This process produces 6 binary-coded-decimal digits.
5
31. Mod-10 subtract each of the 6 binary-coded-decimal digits resulting from Step 30 from the corresponding binary-coded-decimal digit resulting from Step 19.
10
32. Concatenate, left-to-right, (1) the first four digits of the pseudo account number with the second digit (the '9') discarded (thus providing three digits) with (2) the 6 decimal digits resulting from Step 25 with (3) the 6 decimal digits resulting from Step 31. Compute the 16th (right-most) digit by applying the check-digit-generation algorithm to the 15 decimal digits resulting from the concatenation. The resulting 16 digits are the
15 "real" account number.
20

Figures 4a and 4b illustrate the steps that are performed when the cardholder contacts and places an order with a merchant on the Internet and the merchant requests an interchange authorization from an acquirer. It is assumed that the cardholder has enrolled in the MasterCard secure payment program and has
25 installed the MasterCard secure payment application on his/her computer.

- The cardholder contacts a merchant on (for example) the Internet and informs the merchant that he/she wishes to make a purchase.

- The merchant responds by sending to the cardholder a merchant identification number (“MID”) that has been given to it by its acquiring bank (which bank ensures that it gives a unique merchant identification number to each of its merchants), along with a transaction sequence number (“TSN”) that is unique to this transaction. (This response is presumably generated within merchant software that the merchant obtained, for example, (1) from its acquiring bank, and that the acquiring bank had obtained from MasterCard, or (2) from the MasterCard Web site, or (3) from its software vendor, and that this vendor had obtained from MasterCard.) It is assumed that these are decimal numbers and that neither exceeds 8 digits.
- The cardholder executes the MasterCard secure payment application software (if it is not already executing) and enters his/her password.
- The application may display the cardholder’s “real” and pseudo account numbers to the cardholder. The Internet merchants, however, never see the “real” account number.
- The application concatenates the merchant identification number and the transaction sequence number (shown in Figs. 4a and 4b as function “C”), then either:
 1. With reference to Fig. 4a, when the cardholder uses secret-key authentication, the cardholder generates a Message Authentication Code (“MAC”) on the concatenated result, using the unique Per-Card Key placed by MasterCard in the secure payment application (shown in Fig. 4a as function “E2”). As an example of the generation of the MAC, the merchant identification number and the transaction sequence number, represented as binary-coded-decimal, are concatenated, and padded to the right with zeros to produce 16 hexadecimal digits. This is DEA encrypted using, as the key, the left 8-bytes of the Per-Card Key. This result is DEA decrypted using, as the key, the right 8 bytes of the Per-

Card Key, and this second cryptographic result is DEA encrypted using, as the key, the left 8-bytes of the Per-Card Key. Finally the MAC itself is produced by taking the left-most 4 bytes of this 8-byte final result, discarding the right-most 4 bytes. Or:

- 5 2. With reference to Fig. 4b, when the cardholder uses public-key authentication, the cardholder creates a digital signature on the concatenated result of the merchant identification number and the transaction sequence number further concatenated with the transaction amount agreed to by the cardholder (all with appropriate padding) using the card-unique private key placed in the application by MasterCard (or its agent).
- 10 • The MasterCard secure payment application then sends to the merchant, using SSL encryption, the following data:
- 15 1. the cardholder's pseudo account number alone (secret-key authentication) or the card-unique digital certificate (public-key authentication) that includes the card's pseudo account number;
- 20 2. the cardholder's card expiration date;
- 25 3. the merchant identification number and transaction sequence number as received from the merchant;
4. the MAC (secret-key authentication) or the digital signature (public-key authentication) generated by the secure payment application;
5. the transaction amount agreed to by the cardholder.
- In some cases, the secure payment application may also send data in the transaction record indicating that the account number transmitted is a pseudo account number.
- The merchant, using the MasterCard-application software, verifies that the merchant identification number and the transaction sequence number are the correct numbers for this transaction.

- If the transaction uses public-key authentication (Fig. 4b), the merchant, using the MasterCard-application software:
 1. Selects the MasterCard “root” public key indicated by the “root” key identifier in the card’s digital certificate (which public keys are included in the MasterCard application software).
 2. Uses this “root” public key to authenticate the card’s digital certificate.
 3. Uses the card’s public key to authenticate the appropriate transaction data.
 4. Either (a) rejects the transaction if either authentication process fails, or (b) logs all of the data related to the certificate and the transaction signature (so that the merchant can subsequently demonstrate that it successfully verified the certificate and signature).
 - The merchant verifies that the pseudo account number starts with a “5”. The merchant may also verify that the second digit is a “9” for a MasterCard pseudo account number.
 - The merchant may approve the transaction without authorization if that is its practice or it may pass the pseudo account number and card expiration date to the acquiring bank.
- If secret-key authentication is used (see Fig. 4a), the merchant additionally passes to the acquiring bank the merchant identification number, transaction sequence number, and MAC.
- The transaction amount passed from the cardholder to the merchant may be different from the transaction amount passed from the merchant to the acquirer. Therefore, the latter amount is referred to as “authorization amount” in Figs. 4a and 4b.
 - The acquirer receiving the authorization request from the merchant recognizes that it contains a pseudo account number (by the ‘9’ as the second digit, and/or by the inclusion of the fields not found in a conventional authorization request) and sends to its MasterCard-provided security module the pseudo

account number. If secret-key authentication is performed, the acquirer additionally sends to the security module (a) the merchant identification number, (b) the transaction sequence number, and (c) the MAC produced by the cardholder's secure application.

5

- Upon receipt of this data, the security module cryptographically processes the pseudo account number to produce the "real" account number as described above with reference to Fig. 3b. (The translation is shown in Figs. 4a and 4b as using function "D1".)
- If secret-key authentication is required (see Fig. 4a), the security module additionally performs the following steps:
 1. Generates the Per-Card Key, unique to the card of this transaction, using the "real" account number and the Per-Card Key Derivation Key as defined previously. (The generation of the Per-Card Key is shown in Fig. 4a as using function "E3".)
 2. Uses this just-derived key to create a MAC on the merchant identification number and the transaction sequence number, as defined previously.
 3. Compares this generated MAC with the MAC given to it with the transaction data, and rejects the transaction if the two versions of the MAC are not identical.
 4. If the two versions of the MAC are identical, outputs the "real" account number.
- Once the acquirer has obtained the "real" account number from the security module, it combines this with the expiration date from the transaction data. The acquirer may process the resulting transaction internally in its own facility if it is a provider of such processing services, or it may pass the transaction on to MasterCard over Banknet communication

10

15

20

25

30

- lines for MasterCard to send to the issuer in a conventional mode.
- The response received by the acquirer from the issuer is identical in all respects to conventional processing, and provides an approval or rejection based on the “real” account number.
 - If the acquirer passes the account number to the merchant as part of its response, it must first convert the “real” account number back into a pseudo account number using the appropriate cryptographic key stored in the security module, and using the previously-discussed process.

Figure 5 illustrates the process of clearing a transaction. The merchant sends all the transactions to the acquirer at the end of the day or periodically during the day. Each of these transactions includes all of the conventional MasterCard transaction details, except that they may contain a pseudo account number rather than a “real” account number. The acquirer takes all of the pseudo account numbers from these transactions and processes them through the MasterCard-provided security module, thus converting pseudo account numbers to “real” account numbers. The acquirer then processes the transactions internally or routes them to MasterCard International for clearing to the issuer in a conventional manner.

Figure 6 illustrates how charge-backs, retrieval requests, etc., are processed in the MasterCard interchange. The figure shows that both the acquirer and the issuer have security modules 10. However, the issuer need not have a security module unless it will take cardholder inquiries over the Internet and unless the cardholder’s computer communicates with the issuer by outputting a pseudo account number rather than a “real” account number. In this situation the issuer needs a security module in order to be able to convert the pseudo account number to the “real” account number. The issuer does not need a security module if the cardholder communicates with the issuer through postal mail.

The acquirer may have a security module in order to be able to process a transaction as a second presentment or retrieval request fulfillment from a merchant, where the merchant can only reference the transaction with a pseudo account number. Therefore the MasterCard-provided security module at the acquiring bank's facility

- 5 needs the capability to translate from "real" account numbers to pseudo account numbers as well as from pseudo account numbers to "real" account numbers.

The transactions that go through MasterCard will be routed through Banknet with the "real" account number and not the pseudo account number. If secret-key authentication is used, it may be necessary for the acquirer to confirm that
10 the transaction sequence number is unique for the merchant in question. If public-key authentication is used, it may be necessary for the merchant to produce the card's digital certificate, its signature, the cardholder-agreed transaction amount, the merchant identification number and the transaction sequence number, so that it can demonstrate that it actually verified the certificate and signature.

15 When public-key authentication is used, the above discussion considers a one-level key hierarchy in which MasterCard itself directly signs the certificate for every card. However a multi-level hierarchy is also possible. For example, MasterCard might sign a certificate for each of its issuers, and the issuer would in turn sign the certificates for the cards it issued. This would be an example of
20 a two-level hierarchy.

Advantageously, the present invention provides enhanced security for the use of payment account numbers over the Internet. With the present invention, if one or more pseudo account numbers were to be stolen from a merchant, the stolen pseudo account numbers could not be used to conduct fraudulent transactions because
25 transactions based on pseudo account numbers are preferably cryptographically authenticated using a secret key that is unique for each account number. This secret key is located only within the cardholder's secure payment application. Furthermore, a pseudo account number can not be used to make conventional MasterCard

transactions (at point-of-sale terminals, for example) because the pseudo account number does not disclose the "real" account number.

The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise numerous 5 systems and methods which, although not explicitly shown or described herein, embody the principles of the invention and thus within the spirit and scope of the invention.

CLAIMS

1. A method of conducting a transaction by a purchaser over a communications network, comprising:

- (a) assigning to said purchaser a first payment account number having
5 a status which changes over time;
- (b) providing a second payment account number associated with said first payment account number, said second payment account number not being a transaction number and having an encryption key assigned thereto;
- (c) requesting authorization for payment of said transaction with said
10 second payment account number and not said first payment account number;
- (d) identifying said purchaser's first payment account number in response to said authorization request; and
- (e) responding to said authorization request based upon said status of said first payment account number at the time of the transaction.

15 2. The method of claim 1, wherein said authorization request includes a cryptographic code based on said encryption key, and wherein said response to said authorization request is further based on said cryptographic code.

20 3. The method of claim 2, wherein said status is a function of the credit balance available for use by said purchaser, which credit balance changes over time as a result of the purchases made by the purchaser.

4. A method of conducting a transaction by a purchaser over a communications network, comprising:

- (a) assigning to said purchaser a first payment account number having a status which changes over time;
- (b) providing said purchaser with a secure payment application which
25 includes a cryptographic key that is unique to said account number and a pseudo account number having the same length as and associated with said first payment account number;

- (c) providing said purchaser with merchant data based on the transaction;
 - (d) generating a message authentication code as a function of at least said merchant data and said cryptographic key;
 - 5 (e) providing said merchant said pseudo account number and said message authentication code and not said first payment account number;
 - (f) verifying that said merchant data is the correct data for the transaction;
 - (g) requesting an authorization for payment of said transaction, said 10 authorization request not including said first payment account number but including said pseudo account number;
 - (h) recognizing said pseudo account number and cryptographically processing said pseudo account number to produce said first payment account number; and
 - 15 (i) responding to said authorization request based on the status of said first payment account number, and passing said response back without transmission of said first payment account number.
5. The method of claim 4 wherein said pseudo account number is indicated to be different from said first payment account number by a special 20 identifier within the pseudo account number.
6. The method of claim 4 wherein said pseudo account number is indicated to be such by data within a transaction record.
7. The method of claim 4 wherein said cryptographic key is a secret key.
- 25 8. The method of claim 4 wherein said cryptographic key is a private key and said secure payment application further includes a card-unique certificate for the corresponding public key and said message authentication code comprises a digital signature generated by said secure payment application.

9. The method of claim 4 wherein said pseudo account number is obtained by encrypting the associated first payment account number utilizing DESX methodology.

10. The method of claim 4 wherein said pseudo account number is converted back into its associated first payment account number utilizing DEA with a double-length key.

1/9

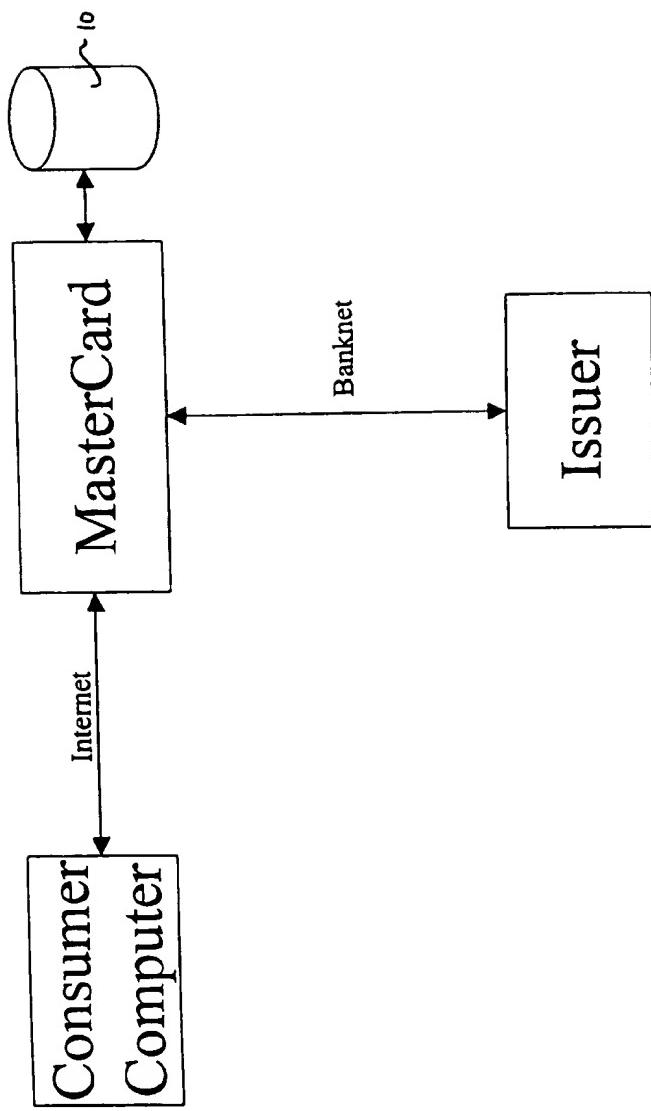


Fig. 1
Consumer Software Initialization

2/9

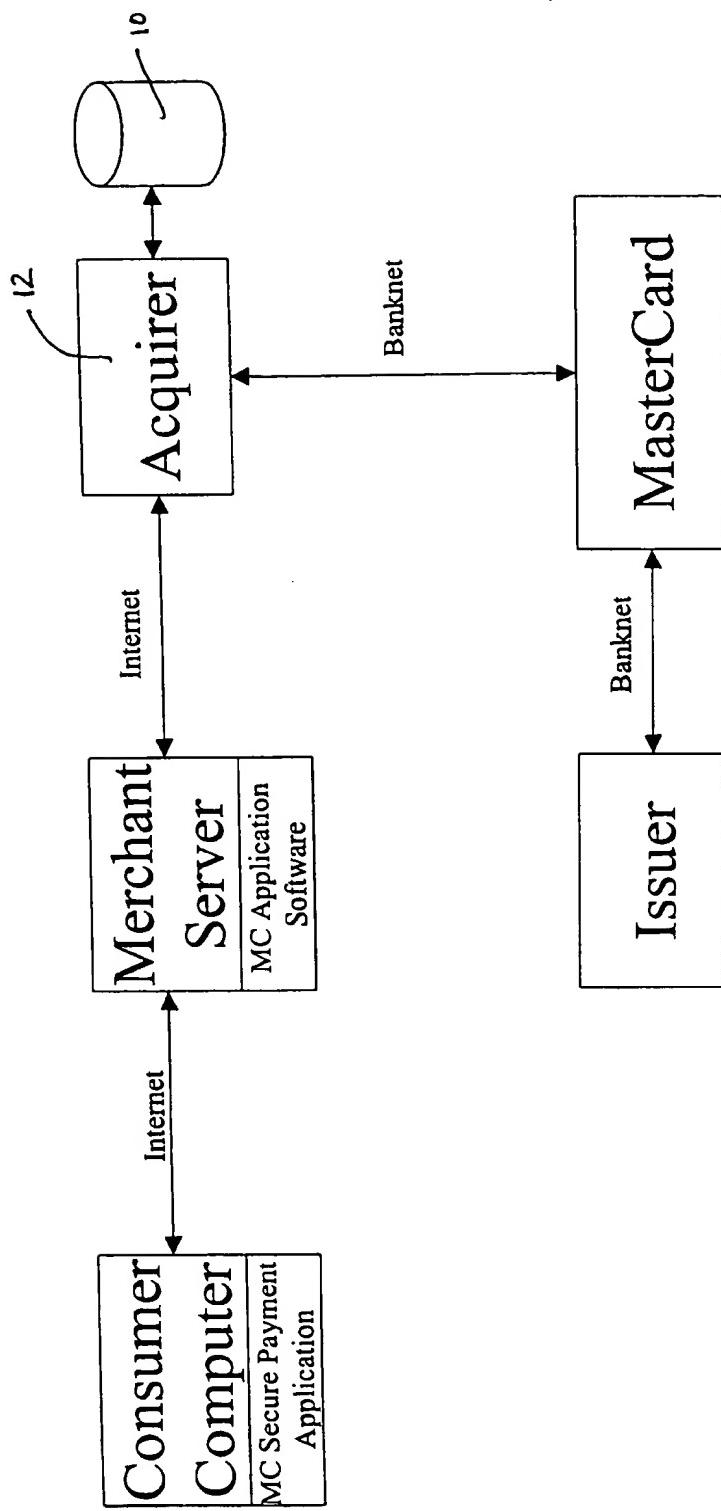


Fig. 2a

Secret Key Authentication

3/9

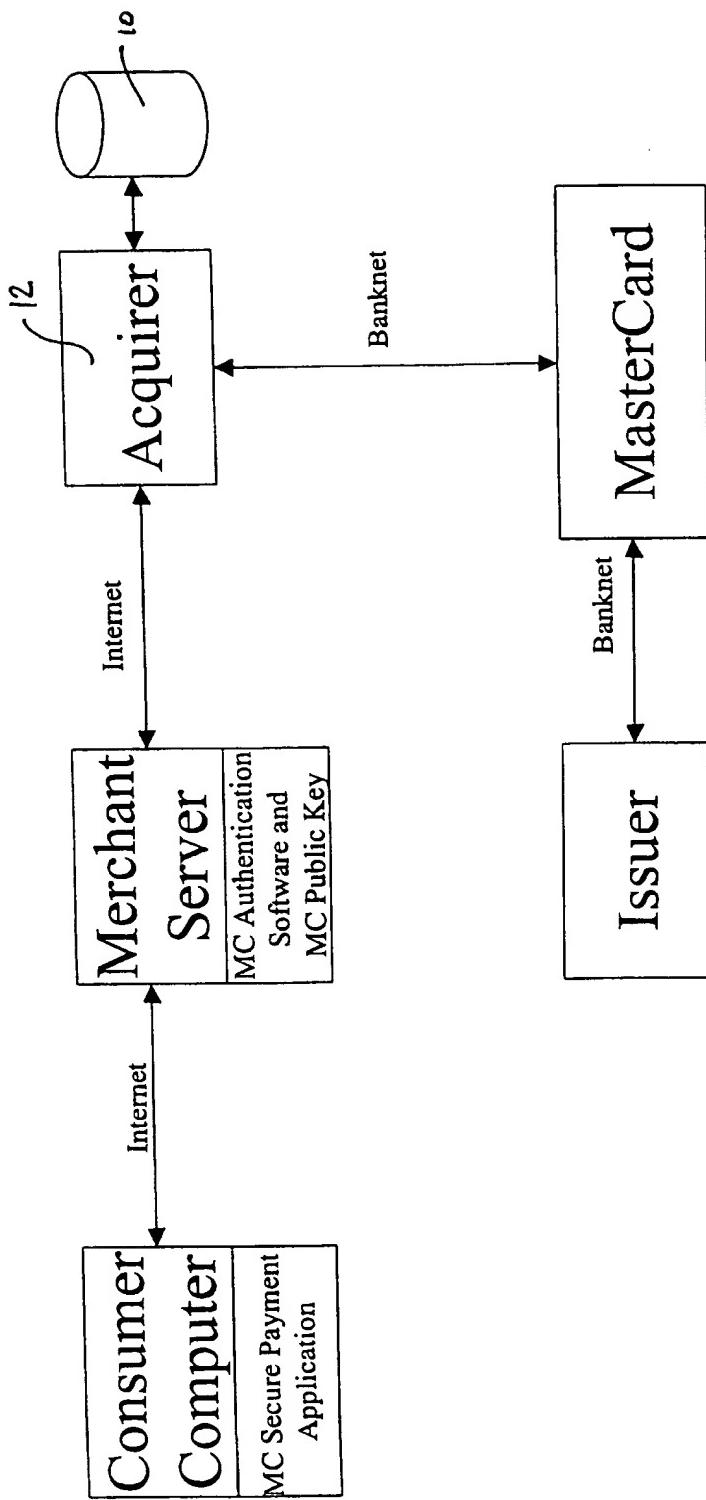


Fig. 2b

Public Key Authentication

4/9

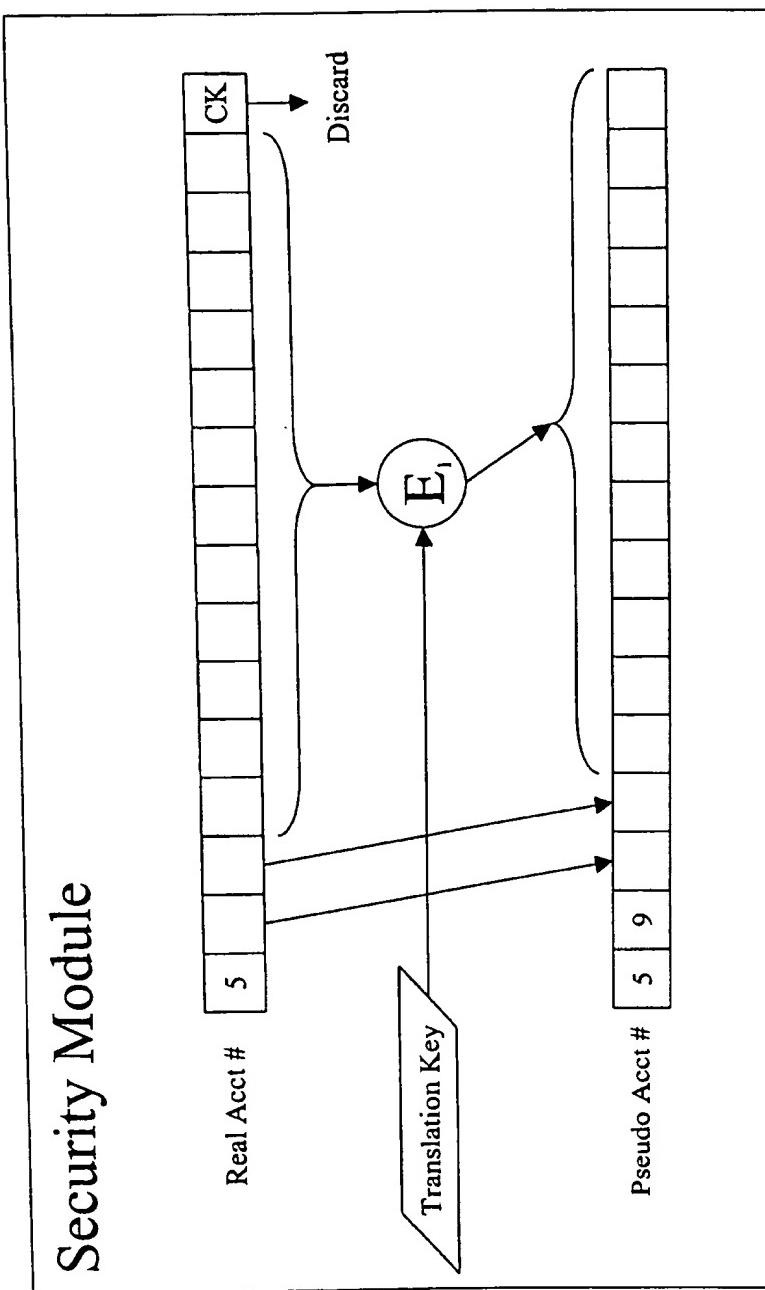


Fig. 3a
Pseudo Acct No. Generation

5/9

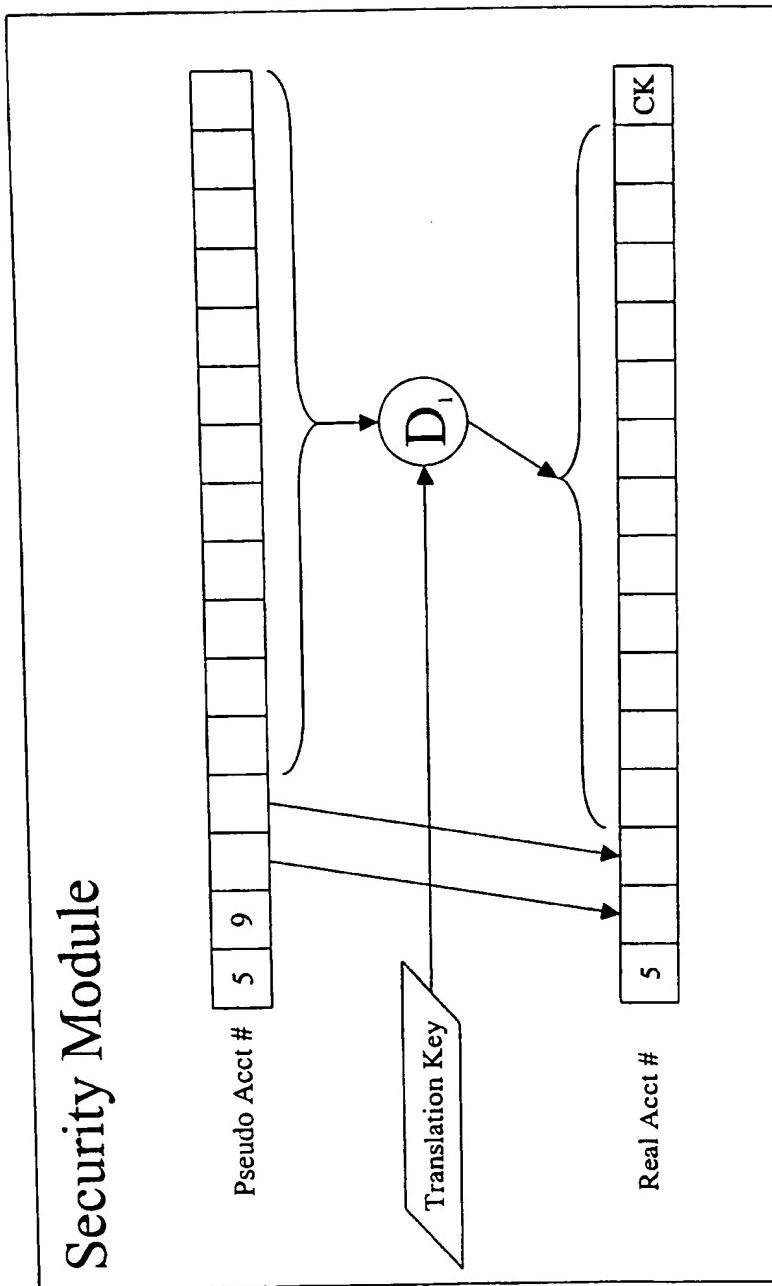


Fig. 3b
Real Acct No. Generation

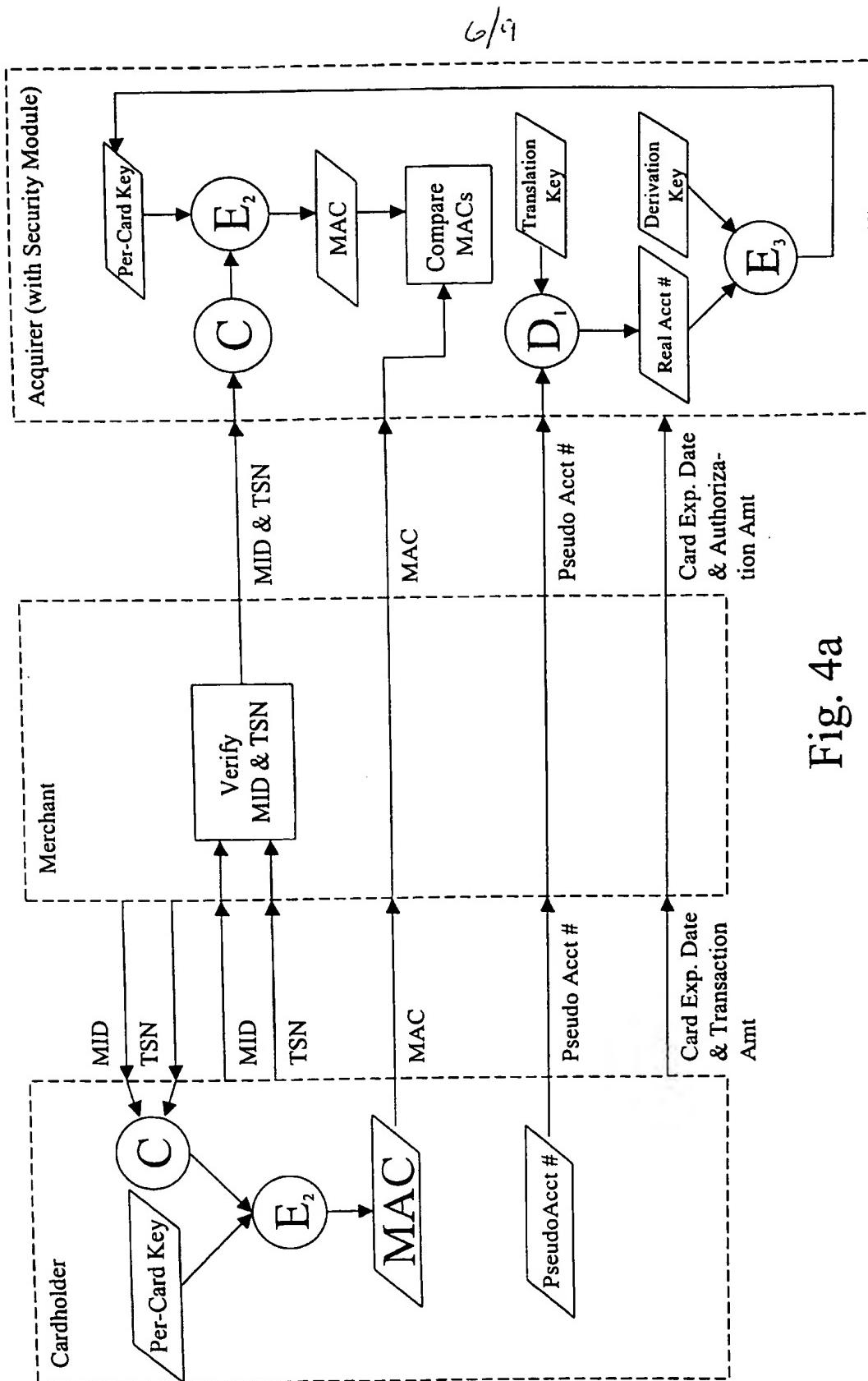


Fig. 4a

Secret Key Authentication

7/9

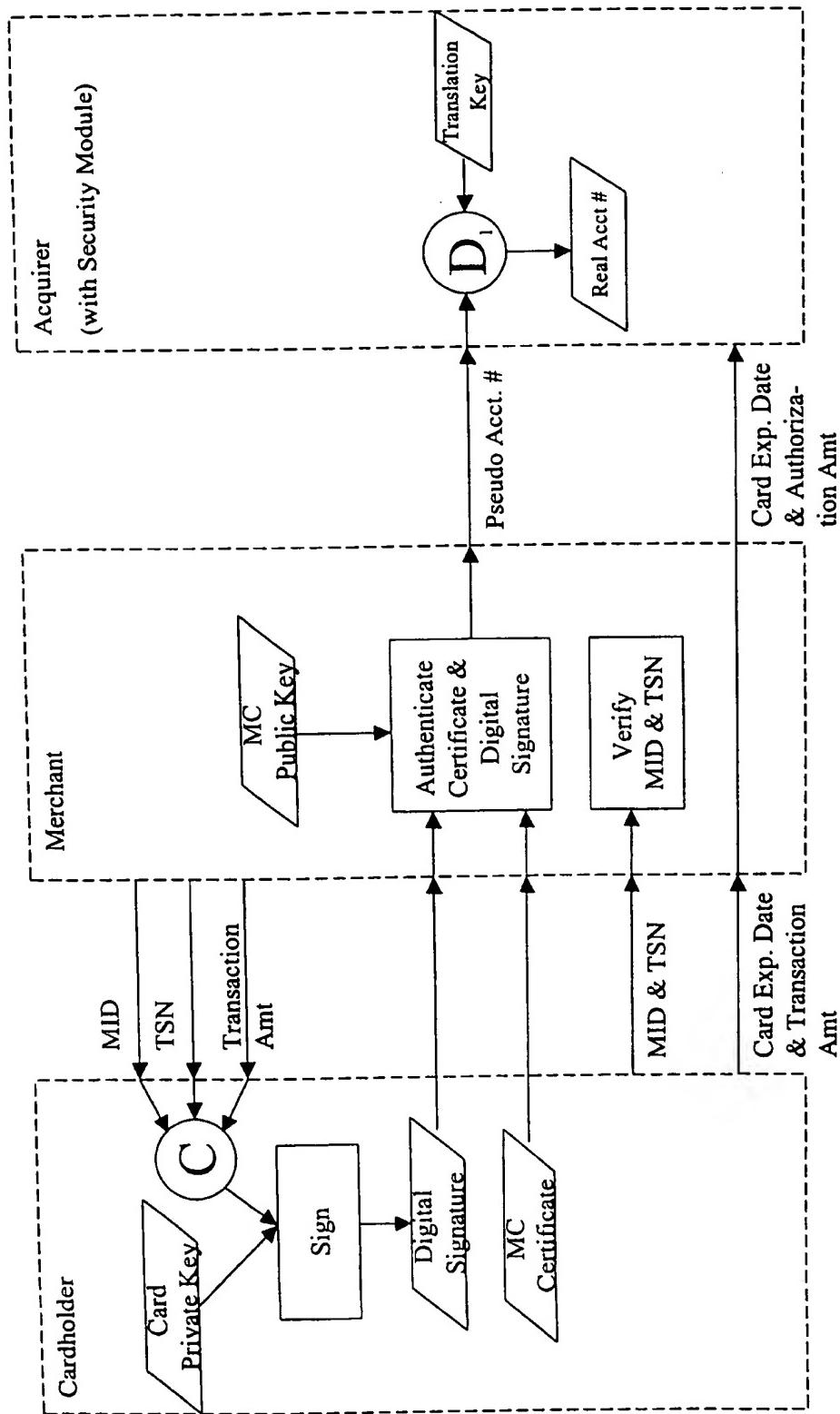


Fig. 4b

Public Key Authentication

8/9

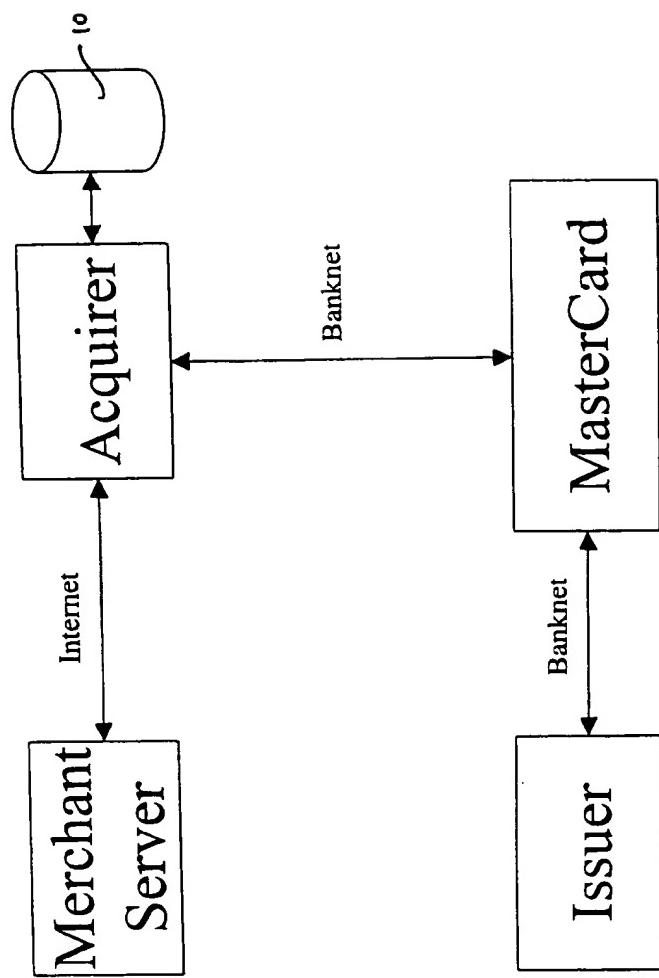


Fig. 5
Clearing & Settlement

9/9

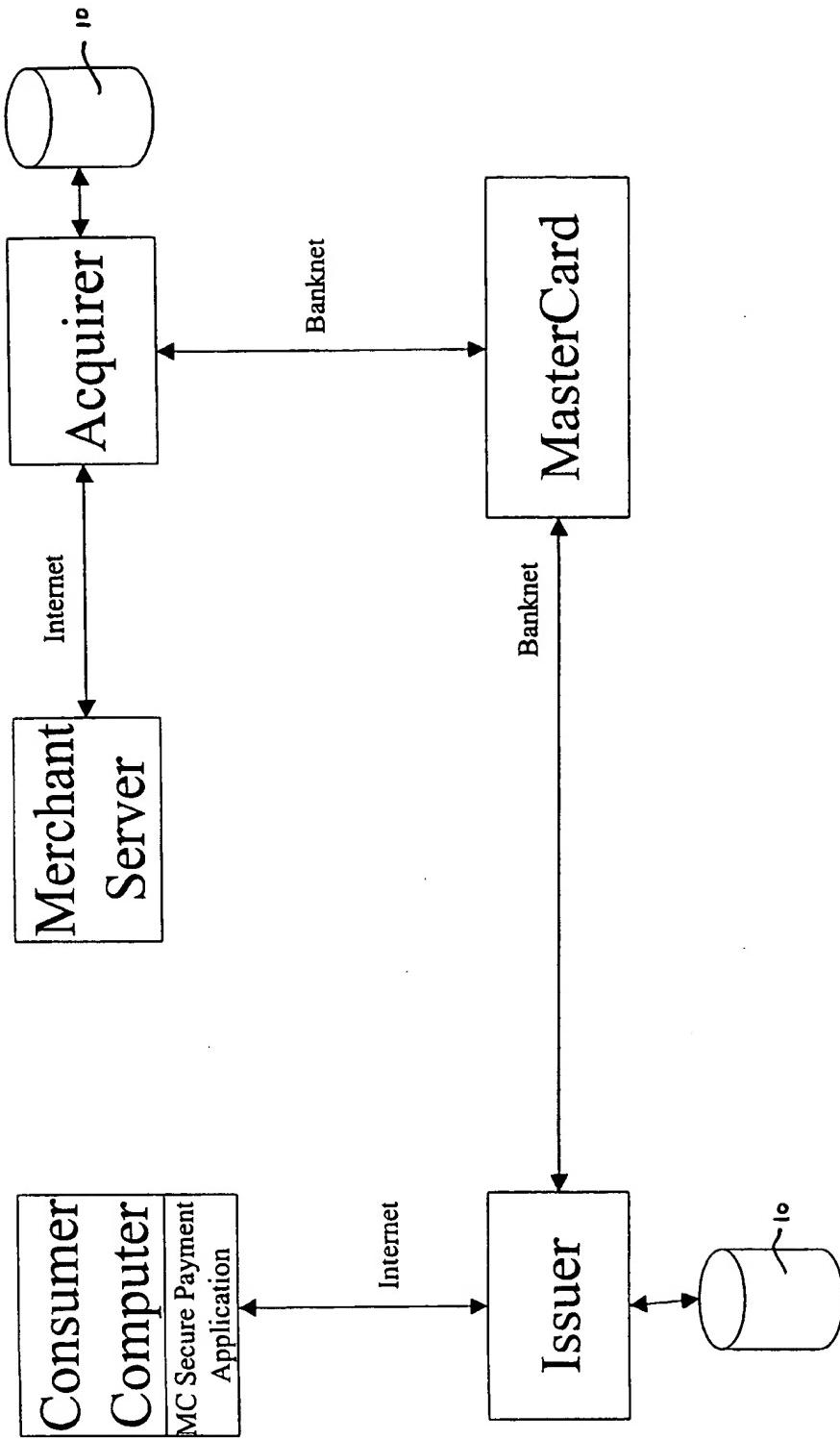


Fig. 6

Exception Processing